Intelligear
Managed Threat Intelligence

External Attack Surface Monitoring

VOLON

CONTENTS

IntelliGear: External Attack Surface Management (EASM)

Volon's External Attack Surface Management (EASM) provides an external outside-in view to identify exposed known and unknown enterprise assets and associated vulnerabilities to help prioritize the most critical issues.

New security requirements have emerged on the back of digital business initiatives such as the shift to cloud infrastructures and remote working, adoption of Internet of Things (IoT) technologies, and IT and OT convergence etc. Volon's EASM will help identify servers, credentials, public cloud service misconfigurations and third-party partner software code vulnerabilities that could be exploited by malicious actors.

EASM Components:

Asset Discovery includes identifying customer domains, sub-domains and their mapping, IP address, subnets and creation of asset exposure register.

Services Discovery includes identifying services running on identified assets including service version and context to the vulnerable services.

Certificate Discovery covers identifying SSL certificates assigned to organization and if any of those are being used by any other site/server

Discovering Misconfigurations that could lead to data leakage. Also it identifies services providing more information than necessary and any code misconfigurations

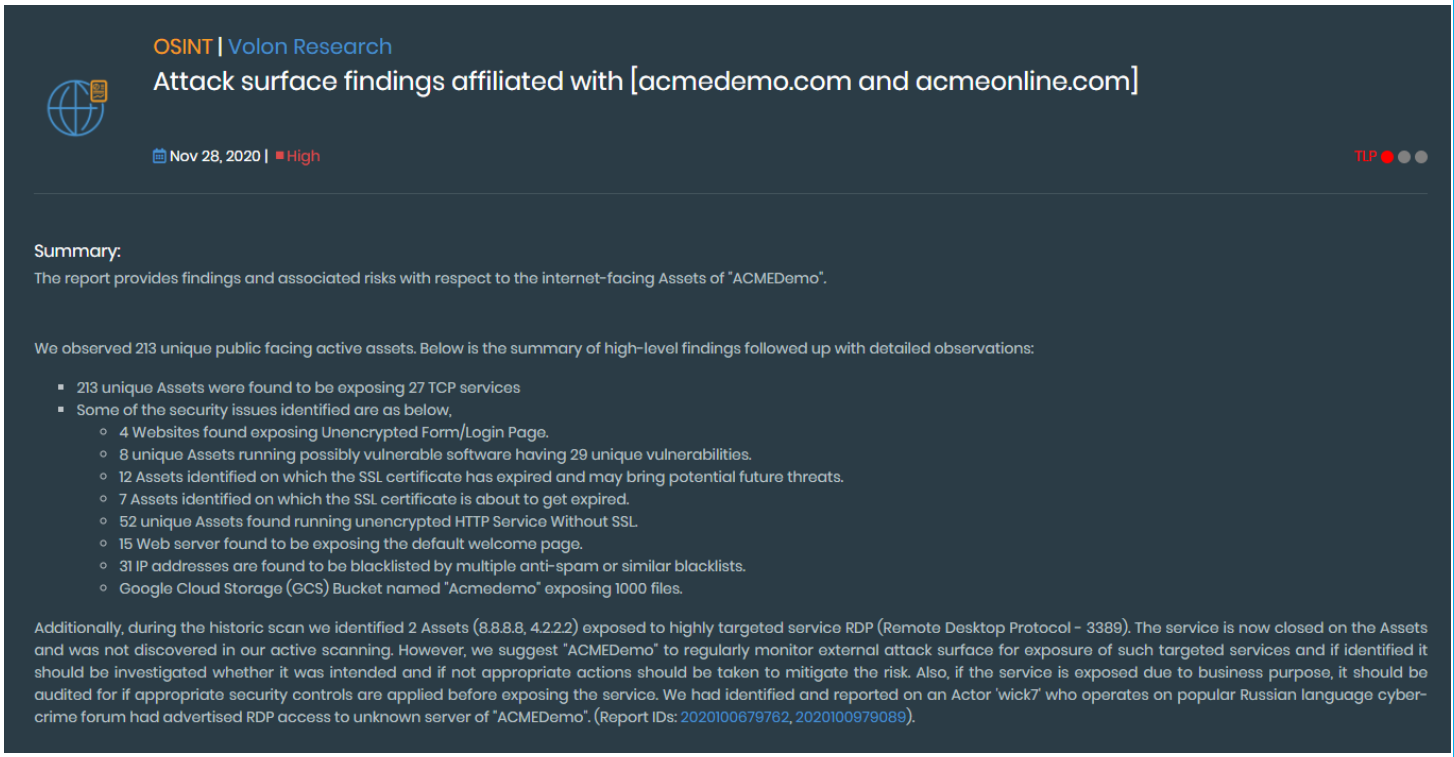
Reputation Checks covers identifying IP address / domain affiliated to customer / brand that may be a part of any Backlists.

EASM will cover the following internet exposed assets:

- Domains/Subdomains
- IP Addresses / Subnets
- Open Ports
- SSL Certificate Scans
- Services
- Possible Misconfigurations
- Reputation Checks

EASM Delivery

Volon deliver EASM Reports to customers via customised portal:



OSINT | Volon Research

Attack surface findings affiliated with [acmedemo.com and acmeonline.com]

Nov 28, 2020 | High

TLP

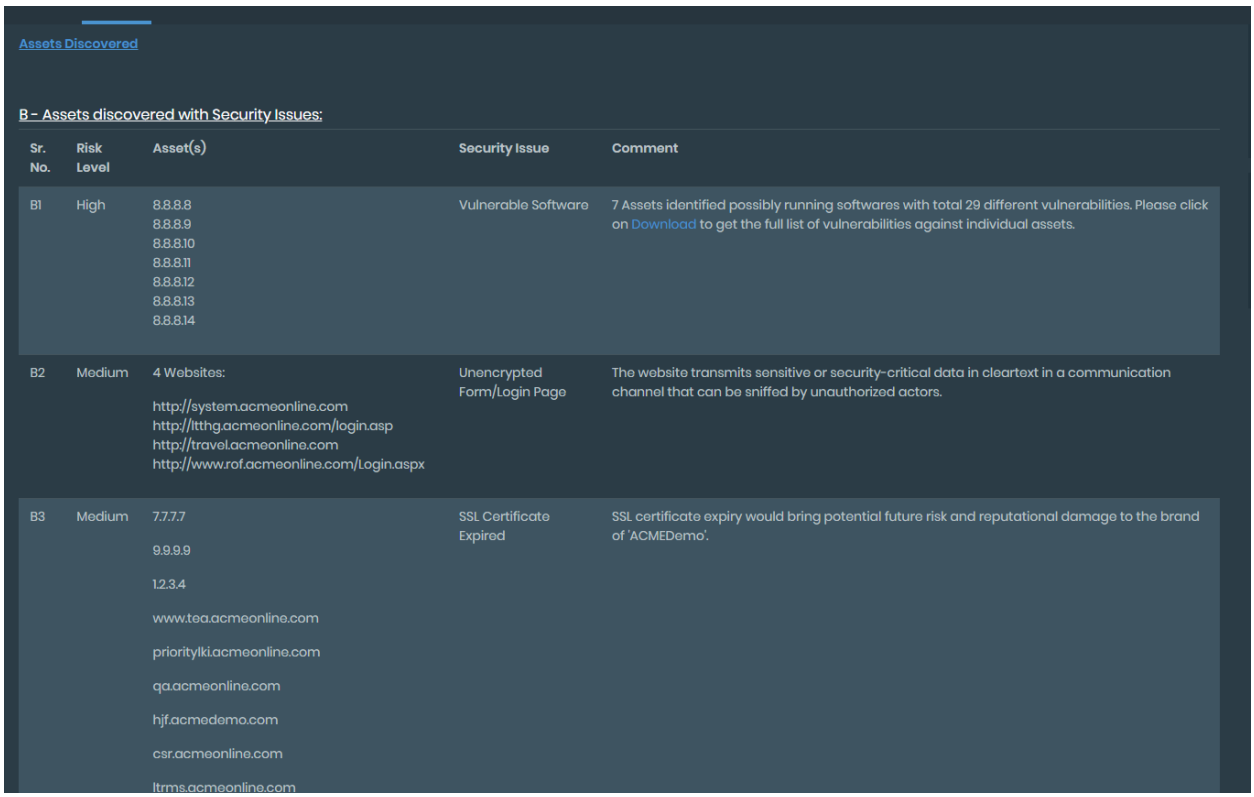
Summary:

The report provides findings and associated risks with respect to the internet-facing Assets of "ACMEDemo".

We observed 213 unique public facing active assets. Below is the summary of high-level findings followed up with detailed observations:

- 213 unique Assets were found to be exposing 27 TCP services
- Some of the security issues identified are as below,
  - 4 Websites found exposing Unencrypted Form/Login Page.
  - 8 unique Assets running possibly vulnerable software having 29 unique vulnerabilities.
  - 12 Assets identified on which the SSL certificate has expired and may bring potential future threats.
  - 7 Assets identified on which the SSL certificate is about to get expired.
  - 52 unique Assets found running unencrypted HTTP Service Without SSL.
  - 15 Web server found to be exposing the default welcome page.
  - 31 IP addresses are found to be blacklisted by multiple anti-spam or similar blacklists.
  - Google Cloud Storage (GCS) Bucket named "Acmedemo" exposing 1000 files.

Additionally, during the historic scan we identified 2 Assets (8.8.8.8, 4.2.2.2) exposed to highly targeted service RDP (Remote Desktop Protocol - 3389). The service is now closed on the Assets and was not discovered in our active scanning. However, we suggest "ACMEDemo" to regularly monitor external attack surface for exposure of such targeted services and if identified it should be investigated whether it was intended and if not appropriate actions should be taken to mitigate the risk. Also, if the service is exposed due to business purpose, it should be audited for if appropriate security controls are applied before exposing the service. We had identified and reported on an Actor 'wick7' who operates on popular Russian language cyber-crime forum had advertised RDP access to unknown server of "ACMEDemo". (Report IDs: 2020100679762, 2020100979089).

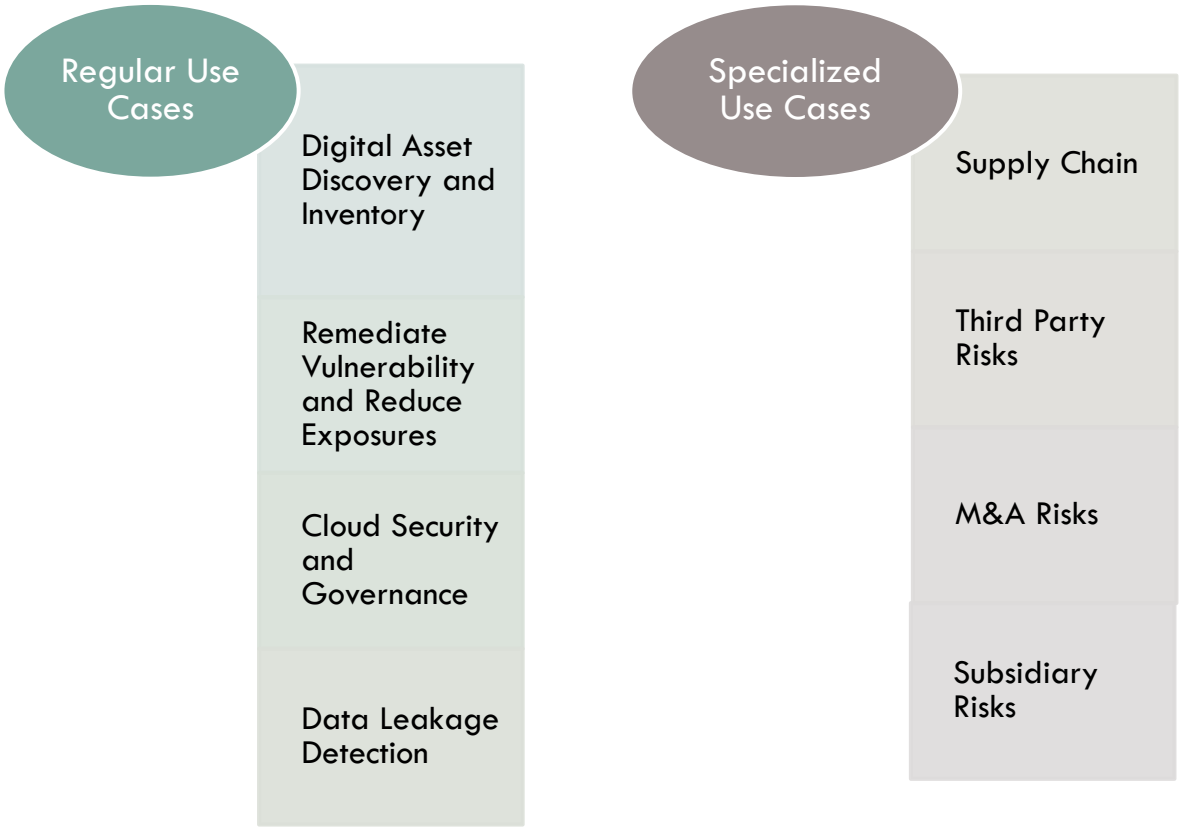


Assets Discovered

B - Assets discovered with Security Issues:

Sr. No.	Risk Level	Asset(s)	Security Issue	Comment
B1	High	8.8.8.8 8.8.8.9 8.8.8.10 8.8.8.11 8.8.8.12 8.8.8.13 8.8.8.14	Vulnerable Software	7 Assets identified possibly running softwares with total 29 different vulnerabilities. Please click on Download to get the full list of vulnerabilities against individual assets.
B2	Medium	4 Websites: http://system.acmeonline.com http://ltthg.acmeonline.com/login.asp http://travel.acmeonline.com http://www.rof.acmeonline.com/Login.aspx	Unencrypted Form/Login Page	The website transmits sensitive or security-critical data in cleartext in a communication channel that can be sniffed by unauthorized actors.
B3	Medium	7.7.7.7 9.9.9.9 1.2.3.4 www.tea.acmeonline.com prioritylki.acmeonline.com qa.acmeonline.com hjf.acmedemo.com csr.acmeonline.com ltrms.acmeonline.com	SSL Certificate Expired	SSL certificate expiry would bring potential future risk and reputational damage to the brand of 'ACMEDemo'.

Volon has wide Use-Case coverage:



VOLON

Volon Cyber Security

www.volon.io